Quantum Key Distribution (QKD) using LEO and MEO Satellites and Decoy States

L. Moli, A. Rodríguez, G. Seco-Granados, J.A. López-Salcedo
Telecommunications and System Engineering Department
Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain.
{Laura.Moli, Ana.Rodriguez, Gonzalo.seco, Jose.Salcedo}@uab.es

***Abstract*—We have analyzed the feasibility of performing Quantum Key Distribution (QKD), in earth-satellite and inter-satellite links, with four quantum cryptography protocols: BB84 and SARG04 with and without decoy states. In order to facilitate the protocols comparison we have computed the rates using the optimal mean photon number for each protocol and for each distance. Furthermore, we have formulate a lower bound on the key generation rate of SARG04 with a finite number of decoy states, and we have obtained all numerical results using realistic values for optical hardware and accounting for realistic atmospheric effects. The results of the analysis indicate that the maximum rate and transmit distance are obtained when the proposed method is applied, and it is possible to establish QKD with LEO (Low Earth Orbit) and MEO (Medium Earth Orbit) satellites.**

I. Introduction

The introduction of satellite technology in the communications has changed the way to understand them, permitting easier and faster communications between each part of the world. From the ancient civilizations the information privacy has been one of the main troubles; the technology development has involved the invention of alternative methods to preserve the security of the communications. Nowadays, the promise of quantum computers breaks the current methods of cryptography. The quantum theory can be applied to cover this loophole. In the last decades the science community has focused its efforts in Quantum Cryptography, developing new quantum cryptography protocols and performing complex experiments and proving that Quantum key distribution (QKD) is the only physically secure way of sharing secret information between two partners. The best known QKD protocol is the BB84, published by Bennett and Brassard in 1984 [1]. Its security is based on the existence of single photon sources. Although there is a strong experimental effort on the design of single photon sources, they are not available yet. At the moment, the best alternative is an attenuated laser source, which provides pulses with a number of photons following a Poisson distribution. The existence of multiple-photon pulses can be exploited by an eavesdropper (Eve). One of the most powerful attacks for the BB84 protocol is the so-called Photon Number Splitting (PNS) attack. In a high-attenuation channel, Eve may extract full information about the key. In order to guarantee security against these attacks, new protocols have appeared: SARG04 [2], B92 [3] and 4+2 protocols [4]. The decoy states method, first proposed by Hwang [5], has represented an important innovation in this area. This method proposes to introduce extra test states (decoy states) to evaluate the action of the eavesdropper. Decoy states method has been successfully applied to the BB84 protocol [6], [7], increasing the achievable distances and the key generation rates. This method has been used in experiments in optical fibers [8], [9] and also in free-space [10]. On the contrary, the application of the decoy states method with protocols other than the BB84 is at best at an early stage. In this paper, we want to contribute to fill this gap proposing a bound of the key generation rate for SARG04 protocol using a finite number of decoy states.

Due to the limitations of the propagation along optical fibres, QKD over fibers can only reach a few hundred of kilometers [11], [12]. Free-space links permit to increase this distance [10] thanks to the low absorption of the atmosphere in certain wavelength ranges and to its nonbirefringent character, which guarantees the conservation of the polarization. However, terrestrial free space links suffer from attenuation caused by the atmosphere and objects in the line of view. In order to totally exploit the potential of free space communications, satellites should be used. Thus, significant improvements in the QKD range could be obtained since, in an earth-satellite link, only around 30 km of the path (depending on the satellite elevation) are inside the atmosphere. The creation of a satellite net will allow a physically secure worldwide net of communications. Up to now, the drawback of satellite quantum cryptography has been the difficulty of performing experiments that demonstrates the feasibility of creating earth-satellite communications, but not long ago the experiment [10] has demonstrate that its is possible to perform quantum cryptography with an attenuation equivalent to the one of earth-satellite links. This result opens the possibility of future experiments using satellites.

The organization of the paper is as follows. In Section II, we describe the link characteristics and the assumptions applicable to the rest of the study. For the sake of completeness, brief analysis of BB84 and SARG04 are provided in Sections III and IV. In Section V, first we review the decoy states method as applied to the BB84 with the vacuum and a weak decoy state. Next, we introduce and analyze our proposal of using SARG04 with the vacuum and two weak decoy states. Section VI contains the numerical results. The last section summarizes the main results and conclusions are drawn.

978-1-4244-2573-0/08/$25.00 ©2008 IEEE

II. Link characteristics

In this section we examine the link characteristics considered for the analysis of quantum channel attenuation. We have assumed that the channel attenuation is caused by beam diffraction, atmospheric attenuation and detector's efficiency. Furthermore, the dark counts of the detector are the only source of the quantum bit error rate (QBER).

A. Photon source and Detector

Quantum cryptography protocols assume that single photon sources are available, but current technology only allow us to generate weak coherent states ($\sqrt{\mu}e^{i\theta}$) using attenuated laser sources. Assuming that the phase of all signals is totally random, the probability distribution for the number of photons follows a Poisson distribution with a parameter μ (mean number of photons per pulse). That is to say, Alice sends an n-photon pulse with a probability $P_n(\mu) = e^{-\mu}\mu^n/n!$. Multi-photon pulses may allow Eve to perform some attacks without being detected by Alice and Bob.

Imperfections in detectors, like low efficiency and dark counts, are some of the main limiting factors in QKD since these factors make the action of an eavesdropper possible. In particular, the low efficiency is one of the main contributions to the attenuation (δ_{det}).

B. Channel attenuation

We assume that conventional telescope architectures, like the Cassegrain type, are used both in the transmitting and receiving sides. They are reflective telescopes, in which the secondary mirror produces a central obscuration. Moreover, their finite dimensions and the distance between them are responsible of the beam diffraction. The attenuation due to beam diffraction and obscuration can be expressed as

$$\delta_{diff} = \left(e^{-2\gamma_t^2\alpha_t^2} - e^{-2\alpha_t^2}\right)\left(e^{-2\gamma_r^2\alpha_r^2} - e^{-2\alpha_r^2}\right), \quad (1)$$
$$\gamma_{t,r} = \frac{b_{t,r}}{\omega}, \qquad \alpha_{t,r} = \frac{R_{t,r}}{\omega}, \qquad \omega(z) \approx \frac{\lambda z}{\pi\omega_0},$$

where the subscript t refers to the transmit telescope and r to the receive one; R and b are the radius of the primary and secondary mirrors, respectively; ω is the waist radius of the Gaussian beam and z is the distance between the telescopes.

Since the atmospheric attenuation (δ_{atm}) is produced by three phenomena: scattering, absorption and turbulence, it can be expressed as $\delta_{atm} = \delta_{scatt}\delta_{abs}\delta_{turb}$. The light is absorbed and scattered by the gas molecules and the aerosols when it passes through the atmosphere. However, the most relevant contribution to the atmospheric attenuation is caused by the turbulence, which is due to thermal fluctuations that produce refractive index variations. The turbulence depends basically on the atmospheric conditions and the position of the ground station. Finally, the total channel attenuation can be written as

$$\delta = \delta_{diff}\delta_{atm}\delta_{det}. \quad (2)$$

III. BB84 Protocol

The BB84 protocol was first proposed by Bennett and Brassard in 1984 [1]. The BB84 protocol consists of two phases: the quantum transmission phase and the classical communication phase. In the first phase, Alice encodes each bit in a qubit using one out of two bases: σ_x or σ_z. The corresponding states can be expressed as: $|+\psi\rangle = 0$, $|-\psi\rangle = 1$; $\psi = x, z$. The qubit is sent to Bob, who measures the qubit randomly using one of the bases. In the second phase, Alice announces by a classical channel the basis that has been used for each qubit. Finally, they use this information to construct the key; a process that involves error correction and privacy amplification.

Due to the fact that real sources generate a portion of pulses having several photons, one of the best possible attacks for Eve against BB84 protocol is the Photon Number Splitting attack (PNS). In the PNS attack, Eve first performs a photon number non-demolition measurement to identify Alice's multi-photon signals. Eve blocks all single photon pulses, while for multi-photon pulses she stores one photon in a quantum memory and reseeds to Bob the remaining photons by a transparent quantum channel.

When Eve realizes the PNS attack, she introduces attenuation. Intuitively, if this attenuation is lower than the channel attenuation, Eve can not be noticed by Alice and Bob, thus she can obtain full information. Note that Eve introduces no errors by performing the PNS attack.

The information shared by Alice and Bob, and that shared by Bob and Eve are given by (in bits/pulse)

$$I(A:B) = \sum_{n=0}^{\infty}\left(1-(1-\delta)^n\right)P_n(\mu) \approx \mu\delta, \quad (3)$$

$$I(B:E) = \sum_{n\geq 2}^{\infty} P_n(\mu). \quad (4)$$

We can define Eve's information as

$$I_{Eve} \triangleq \frac{I(B:E)}{I(A:B)}. \quad (5)$$

A lower bound of the key generation rate is given in [6]:

$$R \geq q\left[-Q_\mu f(E_\mu) H_2(E_\mu) + \Omega\, Q_\mu\left(1 - H_2\left(\frac{E_\mu}{\Omega}\right)\right)\right], \quad (6)$$

where $\Omega = 1 - I_{Eve}$ and q is the efficiency of the protocol (1/2 for BB84), Q_μ is the expected raw rate at Bob's side, $f(x)$ is the bi-directional error correction efficiency (1.22 for the Cascade protocol), H_2 is the binary Shannon entropy, Ω is the fraction of "untagged" photons [1]. E_μ is the QBER and its equal to

$$E_\mu = \frac{Y_0}{2Q_\mu}. \quad (7)$$

Note that the dark counts, Y_0, are the only effect causing the QBER.

[1] "Untagged" refers to the photons from which Eve can not extract information

IV. SARG04 Protocol

In 2004 Scarini et al. presented a new protocol, named SARG04, which is more robust than BB84 against the PNS attack [2]. This protocol is equivalent to the BB84 in the quantum communication phase, while the difference lies in the encoding and decoding of classical information. Instead of communicating the bases, Alice announces publicly one of the four pairs of nonorthogonal states $A_{\omega,\omega'} = \{|\omega x\rangle, |\omega' z\rangle\}$, with $\omega, \omega' \in \{+,-\}$ and with the convention that $|\pm x\rangle = 0,\ |\pm z\rangle = 1$.

Due to the fact that the information is encoded in four nonorthogonal states, when a generalized measure is performed, it is necessary to have at least three copies of the state to obtain a conclusive result with probability P_{ok} [13]. Therefore, to obtain full information Eve must carry out an IRUD attack (Intercept-Resend with Unambiguous Discrimination). The attack starts with a photon number quantum nondemolition measurement; if the pulse contains one or two photons, Eve blocks it, otherwise she realizes a generalized quantum measurement. When the measurement is conclusive, she resends to Bob a copy of the state by a transparent quantum channel.

Eve introduces some attenuation when performing the previous attack. If the channel attenuation is smaller than the introduced by IRUD attack, Eve should adopt a different strategy, otherwise her presence would be immediately detected. In this case, she blocks a fraction t of the single-photon pulses, keeps one photon from two-photon pulses, and she performs the IRUD attack on the rest of the multi-photon pulses. When larger attenuation is possible, all single-photon pulses and a fraction s of the two-photon pulses are blocked. Depending on the value of the attenuation, two regions are possible and are given by

- if $\dfrac{P_2(\mu)+\chi}{\mu} \leq \delta \leq \dfrac{P_1+P_2(\mu)+\chi}{\mu}$,
$$t = 1 - \frac{\delta\mu - P_2(\mu) - \chi}{P_1(\mu)},\ \ s = 0, \quad (8)$$
- if $\dfrac{\chi}{\mu} \leq \delta \leq \dfrac{P_2(\mu)+\chi}{\mu}$,
$$t = 1,\ \ s = 1 - \frac{\delta\mu - \chi}{P_2(\mu)}, \quad (9)$$

where χ is defined as

$$\chi \triangleq \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n). \quad (10)$$

The information shared by Bob and Eve, and that shared by Alice and Bob are given by (in bits/pulse):

$$I(A:B) = P_1(\mu)(1-t) + P_2(\mu)(1-s) + \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n), \quad (11)$$

$$I(B:E) = P_2(\mu) I_2 (1-s) + \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n), \quad (12)$$

where I_2 is the maximum amount of information that Eve can extract from one copy of the state; its value is 0.4 bits/pulse [2]. The value of P_{ok} depends on the number of copies of the state and the overlap of the basis, but it is not less than $1/2$ [13], [14]. Obviously, using this attack, Eve does not obtain information from single photon pulses.

Combining (5), (11) and (12), Eve's information is obtained (see Figure 1). SARG04 shows two different behaviors. The vertex corresponds to $t = 1$ and $s = 0$. Note that SARG04 is better than BB84 since Eve can obtain less information for any distance.

Introducing Eve's information in (6) it is possible to compute the key generation rate for SARG04 protocol. Note that the efficiency (q) of the protocol is $1/4$ for SARG04.

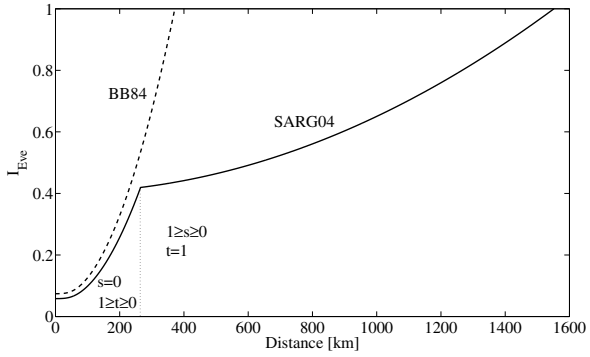

Figure 1. The dashed line shows Eve's information for the BB84 protocol for $\mu = 0.1$. The solid line corresponds to the SARG04 protocol for $\mu = 0.2$.

V. Decoy states method

The decoy-state method was first proposed by Hwang [5], and it has been further studied in [7], [15], [16]. The key point underlying the decoy-states idea is that, using extra test states, the so-called decoy states, a better analysis of the quantum channel or eavesdropping is possible. Signal states (e.g. BB84 or SARG04 states) are used for key generation.
The steps of the decoy states method are as follows:

1) Alice adopts two different kinds of sources: a signal source S with fix mean photon number (μ) and decoy states sources S' with different mean photon numbers $(\nu_1, .., \nu_n)$.
2) Alice randomly chooses the bits value and the sources to encode them.
3) Bob performs the polarization measurement.
4) Alice announces the source used and Bob evaluates the gain of each source. If the gains are different to the expected ones they abort the protocol, otherwise they continue the protocol with signal states.

Next, we discuss the security of the BB84 and the SARG04 protocols using decoy states analyzing the lower bounds of the key generation rates.

A. BB84: Vacuum + weak decoy state

Combining the idea of the entanglement distillation approach in GLLP [17] with the decoy states method, a lower bound for key generation rate was already obtained in [6]:

$$R_{BB84} \geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\}, \tag{13}$$

where Q_μ is the gain of the signal states, E_μ is the QBER, Q_1 is the gain of single-photon states, e_1 is the error rate of single-photon states, and q was already defined in 6. For a coherent state, Q_μ and E_μ are given by

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_n\left(\mu\right), \;\; E_\mu = \frac{\sum_{n=0}^{\infty} Y_n P_n\left(\mu\right) e_n}{Q_\mu}, \tag{14}$$

where Y_n is the yield of the *n*-photon pulses. Y_n is defined as the probability that Bob's measurement is conclusive when Alice emits a *n*-photon pulse and it is given by $Y_n = Y_0 + \delta_n - Y_0\delta_n \cong Y_0 + \delta_n$, where the attenuation for *n*-photon signals is $\delta_n = 1 - (1-\delta)^n$. The error rate of the *n*-photon signals is $e_n = \frac{Y_0}{2Y_n}$.

The values of Q_μ and E_μ can be measured directly from the experiment, whereas Q_1 needs to be bounded based on other gains. The lower bound of Q_1 and the upper bound of e_1, using the Vacuum + weak decoy states method, are given by [7]

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \leq Y_1,$$
$$Q_1^L = \mu e^{-\mu} Y_1^L \leq Q_1, \;\; e_1^U = \frac{e_0 Y_0}{Y_1^L} \geq e_1. \tag{15}$$

The background yield Y_0 can be computed as the gain of the vacuum decoy state. The background error rate e_0 is $1/2$ due to the fact that dark counts occur randomly, so half of the times photons click on the correct detector.

B. SARG04: Vacuum + two weak decoy states

In the BB84 protocol, only single-photon states contribute to the key generation rate. However, in the SARG04 protocol, the key can be generated with both single-photon and two-photon states. Combining this idea with the GLLP [17], the lower bound of key generation rate for SARG04 is [18]

$$R_{SARG04} \geq q\Big\{ - Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right)$$
$$+ Q_1\big[1 - H_2\left(Z_1 \mid X_1\right)\big] + Q_2\big[1 - H_2\left(Z_2\right)\big]\Big\}, \tag{16}$$

where X_n and Z_n represent the bit error and the phase error respectively for *n*-photon. We consider a specific type of Eve's attack, namely the IRUD attack, which does not introduce additional phase or bit errors. All errors are caused by dark counts, which are invariant to the definition of the bases for bit and phase errors. Therefore, we can replace $H_2\left(Z_1 \mid X_1\right)$ for $H_2\left(e_1\right)$.

We put forward a new method to compute the lower bound of the key generation rate in SARG04. It uses three decoy states, ν_0, ν_1, ν_2. Without loss of generality, we assume that ν_0 is the vacuum, and ν_1 and ν_2 are weak decoy states. The bounds of Q_1 and e_1 are obtained as in the BB84 protocol, i.e. using (15) with the vacuum and ν_1 states. Using the decoy states ν_1 and ν_2, it is possible to obtain the following bounds (the proof is omitted for the sake of brevity):

$$Q_2^L = \frac{Y_2^L \mu^2 e^{-\mu}}{2} \leq Q_2 \tag{17}$$

$$e_2^U = \frac{\nu_1 E_{\nu_2} Q_{\nu_2} e^{\nu_2} - \nu_2 E_{\nu_1} Q_{\nu_1} e^{\nu_1} - e_0 Y_0\left(\nu_1 - \nu_2\right)}{Y_2^L \nu_1 \nu_2 \left[\frac{\nu_2 - \nu_1}{2}\right]} \geq e_2. \tag{18}$$

Finally, plugging Q_1^L, Q_2^L, e_1^U and e_2^U in (16) we obtain the lower bound of the key generation rate for the SARG04 protocol with two decoy states.

VI. Numerical results

We have considered three different scenarios: a ground-satellite uplink, a ground-satellite downlink and an intersatellite link. The assumed link parameters are listed in Table I. The wavelength $\lambda = 650$nm corresponds to an absorption window and to an efficiency peak of the chosen detector (an SPCM-AQR-15 commercial silicon avalanche photodiode detector). The values of the telescopes radii have been obtained from the SILEX Experiment [19] and the Tenerife's telescope [20].

Table I
Link parameters

Parameter	Notation	Value
Wavelength	λ	650 nm
Detector efficiency	δ_{det}	65%
Dark counts	Y_0	$50 \cdot 10^{-6}$ counts/pulse
Satellite telescope radius	R	15 cm
Ground telescope radius	R	50 cm
Satellite secondary mirror	b	1 cm
Ground secondary mirror	b	5 cm

The uplink attenuation due to turbulence has been computed considering the Tenerife's telescope ($\backsim$3km above sea level) for two conditions: 1 hour before sunset ($\delta_{turb} = 5$dB) and a typical clear summer day ($\delta_{turb} = 11$dB) [21]. The turbulence effect on the downlink is negligible. The scattering attenuation is evaluated using a model of Clear Standard Atmosphere [22], which results in $\delta_{scatt} = 1$dB.

Figure 2 shows the key generation rates for the studied protocols as a function of the distance. For all protocols, the mean photon number has been optimized to achieve the maximum key generation rate at each distance (see Figure 3). The optimization was carried out by doing an exhaustive search for all possible values of μ and ν_i. Threshold on the minimum values of ν_i was set. It can be seen that optimal values of ν_i are the lowest allowed values. However, these values can not be arbitrarily low since the gains must be quantifiable in a relative short period of time. It means that in that period of time the decoy-state counts must be relevant to estimate the gains with small uncertainty.

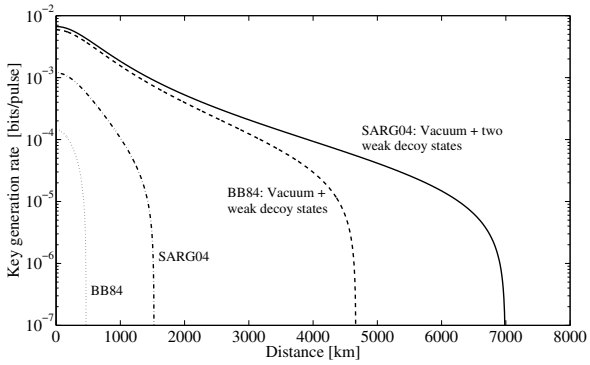

Figure 2. Uplink 1 hour before sunset. The solid line shows SARG04: Vacuum + two weak decoy states, with $\nu_1 = 0.04$ and $\nu_2 = 0.06$. The dashed line shows BB84: Vacuum + weak decoy state, with $\nu = 0.05$. The dotted line shows BB84 protocol. The last line shows SARG04 protocol.

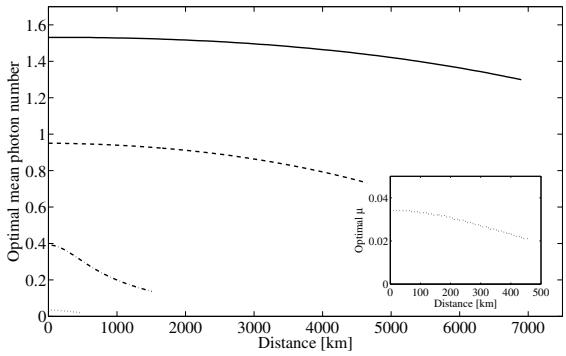

Figure 3. Uplink 1 hr before sunset. The solid line shows SARG04: Vacuum + two weak decoy states. The dashed line shows BB84: Vacuum + weak decoy state. The dotted line shows BB84 protocol, this line is amplified to facilitate the analysis. The last line shows SARG04 protocol.

The critical distance [2] for SARG04 is larger than for BB84. This is due to the fact that SARG04 is more robust than BB84 against eavesdropping (see Figure 1), and it leads to a greater optimal mean photon number. On the other hand, the BB84 critical distance increases significantly when decoy states method is used. It is known that the decoy states method is the most powerful method to increase the critical distances for non-entanglement based protocols. The most drastic improvement occurs when decoy states method is applied to SARG04 protocol, since it achieves the maximum critical distance among all the evaluated protocols. Note that the proposed method is secure when the BB84 with decoy states fails, while for short distances the behaviors are similar.

When the attenuation grows, Eve's attacks are more difficult to be detected hence, the number of multiphoton pulses must be reduced (μ must decrease). This behavior is corroborated by Figure 3. It can also be seen there that the more robust the protocol, the higher value of μ can be used. When the decoy states method is applied, the value of μ remains approximately constant, whereas in the non-decoy protocols it is reduced by a factor of $1/2$ at large distances compared to short distances. The satellites movement along their orbits implies that the distance between them and the ground station or the intersatellite distance vary. In order to achieve the maximal rate at each instant, the value of μ must be modified accordingly, but this is not feasible with current technology. In Figure 4, we compare the optimal rates with the rates obtained when we fix the value of μ to the one that is optimal, for each protocol, at the maximum distance. Actually, the relative decrease is shown. We observe that for decoy protocols the rate decrease is below 3%, which means that the adaptation of the value of μ as a function of the distance is not really necessary. On the contrary, the non-decoy states protocols present significant rate differences, which implies that μ should be adapted to the distance range considered.

The analysis of the other scenarios follows similar steps. Although the values are different, the curves have similar

[2]Maximum distance that can be achieved.

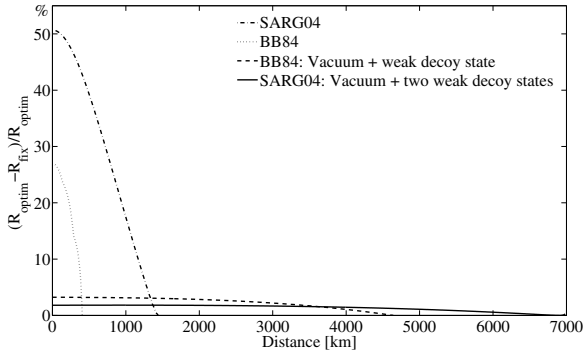

Figure 4. Uplink 1 hr before sunset. Relative difference (in percent) between optimal rate and the rate using a fix μ as a function of the distance.

shapes. Therefore, we only provide the values of the critical distances (Table II) and the maximum rates (Table III). The distances in the downlink are significant larger compared to the uplink thanks to the lack of turbulence attenuation: In fact, MEO satellite downlink communication using SARG04 with decoy states is possible. This increase in distance is not achieved in the intersatellite link due to the reduced telescope dimensions. The most relevant parameters that influence the critical distance are the turbulence attenuation and the telescopes dimensions. Note that for uplink with $\delta_{turb} =$ 11dB is not possible to establish secure communication using the BB84 protocol. Therefore, bidirectional ground-to-LEO satellite communication is only possible with the SARG04 protocol.

An interesting result is to evaluate how much time we need to share a key of 10 bits between European Space Station (400 km) and a ground station. Considering a 10MHz source, SARG04 needs 1ms while SARG04 with decoy states needs only 0.1ms.

It is worth remarking that the proposed method always achieves the maximum rate and transmit distance. The improvement comes basically from the increase of the signal mean photon number and the contribution of two-photon

Table II
CRITICAL DISTANCE [KM]

Scenarios	**BB84**	**SARG04**	**BB84: Vacuum + weak decoy state**	**SARG04: Vacumm + two weak decoy states**
Uplink ($\delta_{turb} = 5$ dB)	460	1520	4650	6980
Uplink ($\delta_{turb} = 11$ dB)	-	500	2200	3460
Downlink	1540	3290	9450	14100
Intersatellite	430	920	2660	3900

Table III
MAXIMUM RATE [BITS/PULSE]

Scenarios	**BB84**	**SARG04**	**BB84: Vacuum + weak decoy state**	**SARG04: Vacumm + two weak decoy states**
Uplink ($\delta_{turb} = 5$ dB)	$1.4 \cdot 10^{-4}$	$1.2 \cdot 10^{-3}$	$5.8 \cdot 10^{-3}$	$6.5 \cdot 10^{-3}$
Uplink ($\delta_{turb} = 11$ dB)	-	$7.5 \cdot 10^{-5}$	$1.4 \cdot 10^{-3}$	$1.6 \cdot 10^{-3}$
Downlink	$1.7 \cdot 10^{-2}$	$2.4 \cdot 10^{-2}$	$4.4 \cdot 10^{-2}$	$4.6 \cdot 10^{-2}$
Intersatellite	$2.0 \cdot 10^{-2}$	$2.6 \cdot 10^{-2}$	$4.8 \cdot 10^{-2}$	$5.0 \cdot 10^{-2}$

pulses to the key generation rate.

VII. CONCLUSIONS

We have presented lower and upper bounds of the key generation rate and the error rate, respectively, for the SARG04 protocol combined with the vacuum and two weak decoy states. The results have been numerically compared with three other protocols: BB84, SARG04 and BB84 using vacuum and one decoy state in realistically modelled ground-satellite and intersatellite links.

It has been shown that SARG04 with decoy states outperforms all other studied cases. Moreover, we have presented the results of optimizing the mean photon number for any distance. Finally, an additional advantage of using decoy states is that an unique value of the signal-state mean photon number is almost optimal in practical terms for all distances.

REFERENCES

[1] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[2] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057901, Feb 2004.

[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[4] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, Mar 1995.

[5] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug 2003.

[6] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005. [Online]. Available: http://link.aps.org/abstract/PRL/v94/e230504

[7] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 72, no. 1, p. 012326, 2005. [Online]. Available: http://link.aps.org/abstract/PRA/v72/e012326

[8] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Physical Review Letters*, vol. 96, no. 7, p. 070502, 2006. [Online]. Available: http://link.aps.org/abstract/PRL/v96/e070502

[9] ——, "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber," in *Proc. IEEE International Symposium on Information Theory*, July 2006, pp. 2094–2098.

[10] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007. [Online]. Available: http://link.aps.org/abstract/PRL/v98/e010504

[11] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev. A*, vol. 65, no. 5, p. 052310, Apr 2002.

[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar 2002.

[13] A. Chefles, "Unambiguous discrimination between linearly independent quantum states," *Phys. Lett. A*, vol. 239, pp. 339–347, 1998.

[14] A. Acín, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, no. 1, p. 012309, Jan 2004.

[15] T. Horikiri and T. Kobayashi, "Decoy state quantum key distribution with a photon number resolved heralded single photon source," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 73, no. 3, p. 032331, 2006. [Online]. Available: http://link.aps.org/abstract/PRA/v73/e032331

[16] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, p. 230503, 2005. [Online]. Available: http://link.aps.org/abstract/PRL/v94/e230503

[17] D. Gottesman, H.-K. LO, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information Computing*, vol. 5, p. 325, 2004. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0212066

[18] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum-key-distribution protocols," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 73, no. 1, p. 012337, 2006. [Online]. Available: http://link.aps.org/abstract/PRA/v73/e012337

[19] P. Gatenby and M. Grant, "Optical intersatellite links," *Electronics and Communication Engineering Journal*, vol. 3, no. 6, pp. 280–288, Dec 1991.

[20] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nat Phys*, vol. 3, no. 7, pp. 481–486, 2007. [Online]. Available: http://dx.doi.org/10.1038/nphys629

[21] D. G. Aviv, *Laser Space Communications*. Artech House, 2006.

[22] L. Elterman, "Parameters for attenuation in the atmospheric windows for fifteen wavelengths," *Appl. Opt.*, vol. 3, no. 6, pp. 745–749, 1964. [Online]. Available: http://ao.osa.org/abstract.cfm?URI=ao-3-6-745